Intro Cryptography (Day 2)

1. Review *shift ciphers*: What is the key in the shift cipher below? KEY: 11

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
in	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
out	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K

2. A shift cipher is a particular type of substitution cipher. Below is a substitution cipher that is **not** a shift cipher.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
in	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
out	E	F	G	L	8	A	R	Q	T	U	V	P	B	D	N	O	H	M
	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35
in	S	T	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9
out	I	1	4	7	J	6	5	K	9	3	2	0	C	X	S	Z	Y	W

(a) Encrypt: MEET APRIL 3
B881EOMTP0 ← you have to be clear about the letter oh "O" and the number zero "0"

(b) Decrypt: F4IE19Z09
BUSAT073Ø = Bus at 7:30.

(c) What key is needed to decrypt a message using this encryption scheme?
You need the whole table.

(d) Which substitution is, in general, harder to break, a shift cipher or one that is not a shift cipher?
the non-shift cipher. in a shift cipher, you know one letter you know them all.

(e) What strategies would you use to try to break a substitution cipher that is not a shift cipher?
letter frequencies and guessing words.

3. Another encryption scheme is called a **transposition cipher**.

Encode JEWEL FOUND using a transposition cipher of rows of 4 letters.

Write letters in rows

J	E	W	E
L	F	O	U
N	D	Z	W

make this up

Rewrite as columns

JLNEFDWOZEUW

Key: row length.